International Journal of Bifurcation and Chaos

Breaking an image encryption algorithm based on chaos

Chengqing Li
Department of Electronic and Information Engineering,
The Hong Kong Polytechnic University, Hong Kong
chengqing8@gmail.com

Michael Z. Q. Chen
Department of Mechanical Engineering,
The University of Hong Kong, Hong Kong

Kwok-Tung Lo
Department of Electronic and Information Engineering,
The Hong Kong Polytechnic University, Hong Kong

July 22, 2010

Recently, a chaos-based image encryption algorithm called MCKBA (Modified Chaotic-Key Based Algorithm) was proposed. This paper analyzes the security of MCKBA and finds that it can be broken with a differential attack, which requires only four chosen plain-images. Performance of the attack is verified by experimental results. In addition, some defects of MCKBA, including insensitivity with respect to changes of plain-image/secret key, are reported.

Keywords: image; encryption; chaos; differential attack.

1. Introduction

Rapid development of information technology and popularization of digital products require that multimedia data are transmitted over all kinds of wired/wireless networks more and more frequently. Therefore, secure delivery of multimedia data becomes increasingly important. However, traditional text encryption schemes fail to be competent for the task due to the big differences between textual and multimedia data. Under the pressure of this challenge, researchers attempted to propose special multimedia encryption schemes utilizing all kinds of nonlinear theories in the past decade. The subtle similarity between chaos and cryptography makes chaos considered as an ideal tool to design secure and efficient encryption schemes and a great number of multimedia encryption schemes based on it have been presented [Chen & Yen, 2003; Chen *et al.*, 2004; Pisarchik *et al.*, 2006; Xiang *et al.*, 2007; Ye, 2010; Wong *et al.*, 2010]. Unfortunately, many of them have been found to be insecure and/or incomplete from the viewpoint of modern cryptology [Wang *et al.*, 2005; Li *et al.*, 2008b,a; Arroyo *et al.*, 2008; Zhou & Au, 2008; Ercan & Cahit, 2009; Li *et al.*, 2009b,a; Solak *et al.*, 2010]. References [Álvarez & Li, 2006; Li *et al.*, 2004] conclude some general rules about evaluating the security of chaos-based encryption schemes.

In [Yen & Guo, 2000], a chaotic key-based algorithm (CKBA) for image encryption was proposed. The algorithm encrypts each pixel by four possible operations: XORing or XNORing it with one of two predefined sub-keys. A pseudo-random number sequence (PRNS), obtained from a one-dimensional chaotic

system, is used to determine which operation is exerted. As shown in [Li & Zheng, 2002], CKBA can be easily broken with only one known/chosen-image. To enhance security of CKBA against known/chosen-plaintext attack, [Rao & Gangadhar, 2007] proposes a modified chaotic-key based algorithm (MCKBA) by employing a modular addition operation like [Socek *et al.*, 2005]. To further enhance the security against brute-force attack, [Gangadhar & Rao, 2010] replaces the one-dimensional chaotic system generating PRNS with a simple hyperchaos generator proposed in [Takahashi *et al.*, 2004] and names the algorithm HCKBA (Hyper Chaotic-Key Based Algorithm). Since the two schemes MCKBA and HCKBA share the same structure, this paper only analyzes the security of MCKBA and finds that the scheme can be broken with only four chosen plain-images. Both theoretical analysis and experimental results are provided to support the conclusion. In addition, some other security defects of MCKBA, including insensitivity with respect to changes of plain-image/secret key, are discussed.

The rest of this paper is organized as follows. The image encryption algorithm under study is introduced in Sec. 2. Detailed cryptanalysis on the algorithm is presented in Sec. 3 with experimental results. The last section concludes this paper.

2. Modified Chaotic-Key Based Algorithm (MCKBA)

The plaintext encrypted by MCKBA is a gray-scale image of size $M \times N$ (width$\times$height). The plain-image is scanned in the raster order and represented as a 1D signal $\boldsymbol{I} = \{I(i)\}_{i=0}^{MN-1}$. Then, a binary sequence $\boldsymbol{I}_b = \{I_b(l)\}_{l=0}^{8MN-1}$ is constructed, where $\sum_{j=0}^{7} I_b(8 \cdot i + j) \cdot 2^j = I(i)\ \forall\ i \in \{0, \cdots, MN-1\}$. With a pre-defined integer parameter n, an n-bit number sequence $\boldsymbol{J} = \{J(i)\}_{i=0}^{\lceil 8MN/n \rceil -1}$ is generated for encryption, where $J(i) = \sum_{j=0}^{n-1} I_b(n \cdot i + j) \cdot 2^j$. Note that sequence $\boldsymbol{I}_b$ is padded with some zero bits if $(8MN)$ is not a multiple of n. Without loss of generality, assume n can divide $(8MN)$ here. MCKBA operate on the intermediate sequence $\boldsymbol{J}$ and get $\boldsymbol{J}' = \{J'(i)\}_{i=0}^{8MN/n-1}$, where $J'(i) = \sum_{j=0}^{n-1} I'_b(n \cdot i + j) \cdot 2^j$. Finally, cipher-image $\boldsymbol{I}' = \{I'(i)\}_{i=0}^{MN-1}$ is obtained, where $I'(i) = \sum_{j=0}^{7} I'_b(8 \cdot i + j) \cdot 2^j$. With the above notations, MCKBA can be described as follows[1].

- *The secret key*: two random numbers $key_1, key_2 \in \{0, \cdots, 2^n - 1\}$, and the initial condition $x(0) \in (0, 1)$ of the following chaotic Logistic map:
$$x(i+1) = 3.9 \cdot x(i) \cdot (1 - x(i)), \tag{1}$$
where $\sum_{j=0}^{n-1}(key_{1,j} \oplus key_{2,j}) = \lceil n/2 \rceil$, $key_1 = \sum_{j=0}^{n-1} key_{1,j} \cdot 2^j$, $key_2 = \sum_{j=0}^{n-1} key_{2,j} \cdot 2^j$, and $\oplus$ denotes eXclusive OR (XOR) operation.
- *Initialization*: run the chaotic system to generate a chaotic sequence, $\{x(i)\}_{i=0}^{MN/(2n)-1}$. From the 32-bit binary representation of $x(i) = \sum_{j=1}^{32} b(32 \cdot i + j - 1) \cdot 2^{-j}$, derive a pseudo-random binary sequence (PRBS), $\{b(l)\}_{l=0}^{16MN/n-1}$.
- *Encryption*: for the i-th plain-element $J(i)$, $i = 0 \sim 8MN/n - 1$, the corresponding cipher-element $J'(i)$ is determined by the following rule:
$$J'(i) = \begin{cases} (J(i) \dot{+} key_1) \oplus key_1, & \text{if } B(i) = 3, \\ (J(i) \dot{+} key_1) \odot key_1, & \text{if } B(i) = 2, \\ (J(i) \dot{+} key_2) \oplus key_2, & \text{if } B(i) = 1, \\ (J(i) \dot{+} key_2) \odot key_2, & \text{if } B(i) = 0, \end{cases} \tag{2}$$
where $B(i) = 2 \cdot b(2i) + b(2i+1)$, $a \dot{+} b = (a + b) \bmod 2^n$ and $\odot$ denotes XNOR operation. Since

[1] To make the presentation more concise and consistent, some notations in the original paper [Rao & Gangadhar, 2007] are modified, and some details of MCKBA are also supplied.

$a \odot b = \overline{a \oplus b} = a \oplus \bar{b}$, the above equation is equivalent to

$$J'(i) = \begin{cases} (J(i) \dotplus key_1) \oplus key_1, & \text{if } B(i) = 3, \\ (J(i) \dotplus key_1) \oplus \overline{key_1}, & \text{if } B(i) = 2, \\ (J(i) \dotplus key_2) \oplus key_2, & \text{if } B(i) = 1, \\ (J(i) \dotplus key_2) \oplus \overline{key_2}, & \text{if } B(i) = 0. \end{cases} \tag{3}$$

- *Decryption*: the decryption procedure is similar to that of the encryption, but with Eq. (3) replaced by following

$$J(i) = \begin{cases} (J'(i) \oplus key_1) \dot{-} key_1, & \text{if } B(i) = 3, \\ (J'(i) \oplus \overline{key_1}) \dot{-} key_1, & \text{if } B(i) = 2, \\ (J'(i) \oplus key_2) \dot{-} key_2, & \text{if } B(i) = 1, \\ (J'(i) \oplus \overline{key_2}) \dot{-} key_2, & \text{if } B(i) = 0, \end{cases} \tag{4}$$

where $a \dot{-} b = (a - b + 2^n) \bmod 2^n$.

3. Cryptanalysis

3.1. *The Differential Attack*

Differential attack is usually a chosen-plaintext attack, assuming that the attacker can obtain cipertexts for some set of chosen plaintexts. The goal of the attack is to gain information about the secret key or plaintext by analyzing how differences in the chosen plaintexts affect the resultant difference at the corresponding ciphertexts. Note that difference is defined with respect to any given operation, e.g., XOR. In [Rao & Gangadhar, 2007, III.B] and [Gangadhar & Rao, 2010, Sec. 3.2], the authors claimed that MCKBA is very robust against chosen-plaintext attack. However, we will show how it can be broken very easily with only four chosen plain-images.

Since plain-image and intermediate sequences $\boldsymbol{J}$ can be obtained from each other without any secret key, choosing the former is actually equivalent to choosing the latter. If two known intermediate sequences $\boldsymbol{J}_1 = \{J_1(i)\}_{i=0}^{8MN/n-1}$ and $\boldsymbol{J}_2 = \{J_2(i)\}_{i=0}^{8MN/n-1}$ are encrypted with the same secret key, their corresponding encrypted results $\boldsymbol{J}'_1 = \{J'_1(i)\}_{i=0}^{8MN/n-1}$ and $\boldsymbol{J}'_2 = \{J'_2(i)\}_{i=0}^{8MN/n-1}$ satisfy the following relation

$$J'_1(i) \oplus J'_2(i) = \begin{cases} (J_1(i) \dotplus key_1) \oplus (J_2(i) \dotplus key_1), & \text{if } B(i) = 3, \\ (J_1(i) \dotplus key_1) \oplus (J_2(i) \dotplus key_1), & \text{if } B(i) = 2, \\ (J_1(i) \dotplus key_2) \oplus (J_2(i) \dotplus key_2), & \text{if } B(i) = 1, \\ (J_1(i) \dotplus key_2) \oplus (J_2(i) \dotplus key_2), & \text{if } B(i) = 0. \end{cases} \tag{5}$$

Regardless the value of $B(i)$, $(J'_1(i) \oplus J'_2(i))$ can be represented by an equation in the following form

$$y = (a \dotplus x) \oplus (b \dotplus x), \tag{6}$$

where $a, b, x, y \in \{0, \cdots, 2^n - 1\}$.

The following theorem discusses how to solve the above equation.

Theorem 1. *Assume that a, b, x are all n-bit integers, then a lower bound on the number of queries (a, b) to solve Eq. (6) for any x is (i) 0 if $n = 1$; (ii) 1 if $n = 2$; (iii) 2 if $n = 3$; or (iv) 3 if $n \geq 4$.*

Proof. First, rewrite Eq. (6) as the following equivalent form

$$\tilde{y} = y \oplus a \oplus b = (a \dotplus x) \oplus (b \dotplus x) \oplus a \oplus b. \tag{7}$$

Let $x = \sum_{j=0}^{n-1} x_j \cdot 2^j$, $a = \sum_{j=0}^{n-1} a_j \cdot 2^j$, $b = \sum_{j=0}^{n-1} b_j \cdot 2^j$, and $\tilde{y} = \sum_{j=0}^{n-1} \tilde{y}_j \cdot 2^j$. Then, except $\tilde{y}_0 \equiv 0$, Eq. (7) can be decomposed into the following iteration form

$$\begin{cases} c_{i+1} = (x_i \cdot a_i) \oplus (x_i \cdot c_i) \oplus (a_i \cdot c_i), \\ \tilde{c}_{i+1} = (x_i \cdot b_i) \oplus (x_i \cdot \tilde{c}_i) \oplus (b_i \cdot \tilde{c}_i), \\ \tilde{y}_{i+1} = c_{i+1} \oplus \tilde{c}_{i+1}, \end{cases} \tag{8}$$

where $i \in \{0, \cdots, n-2\}$, $c_0 = 0$, $\tilde{c}_0 = 0$.

Table 1 lists the values of $\tilde{y}_{i+1}$ under all possible different values of $a_i, b_i, \tilde{y}_i, x_i, c_i$. From Table 1, one can see that the values of unknown bit x_i can be determined if and only if $(a_i, b_i, \tilde{y}_i)$ falls in the 1, 2, 4, 7-th column (zero-based) of the table, namely

$$(a_i + b_i \cdot 2 + \tilde{y}_i \cdot 2^2) \in \{1, 2, 4, 7\}. \tag{9}$$

Table 1. The values of $\tilde{y}_{i+1}$ corresponding to the values of $a_i, b_i, \tilde{y}_i, x_i, c_i$.

(x_i, c_i) \ $(a_i, b_i, \tilde{y}_i)$	(0,0,0)	(0,0,1)	(0,1,0)	(0,1,1)	(1,0,0)	(1,0,1)	(1,1,0)	(1,1,1)
(0, 0)	0	0	0	1	0	0	0	1
(0, 1)	0	0	1	0	1	1	0	1
(1, 0)	0	1	1	1	1	0	0	0
(1, 1)	0	1	0	0	0	1	0	0

When $n = 1$, Eq. (7) becomes $\tilde{y} \equiv 0$. So, no pair of (a, b) is required to achieve the value of x. Since $\tilde{y}_{n-1}$ bears no relation with x_{n-1}, we only need to discuss how to obtain the $(n-1)$ least significant bits of x for other values of n.

- $n = 2$: Since $\tilde{y}_0 = 0$, $c_0 = 0$, one can get $x_0 = \tilde{y}_1$ by setting $(a_0, b_0) = (1, 0)$;
- $n = 3$: No matter what (a_0, b_0) is, $y_1 \in \{0, 1\}$. Therefore, it is impossible to obtain x_1 with only set of (a_1, b_1) for any x. Select (a, b) satisfying that $(a_0, b_0) = (1, 0)$, get x_0 as the above case. Let $(a_1, b_1) = (1, 0)$, x_1 can be determined if $y_1 = 0$; otherwise we have to resort to another query (a', b'). Let $\tilde{y}' = \sum_{j=0}^{n-1} \tilde{y}'_j \cdot 2^j$ denote the output of Eq. (7) corresponding to the second query. Set $(a'_0, b'_0) = (a_0, b_0)$ and $(a'_1, b'_1) = (1, 1)$ if $y_1 = 1$, then we can get $x_1 = \overline{y'_2}$;
- $n \geq 4$: In this case, $(\tilde{y}_1, \tilde{y}_2)$ and $(\tilde{y}'_1, \tilde{y}'_2)$ can be all possible values. Observing Table 1, it can be easily verified that there is no (a, b) and (a', b') satisfying either Eq. (9) or

$$(a'_i + b'_i \cdot 2 + \tilde{y}'_i \cdot 2^2) \in \{1, 2, 4, 7\} \tag{10}$$

for $i = 1, 2$. This means x_2 cannot always be determined. Therefore, we need one more query $(a^\star = \sum_{j=0}^{n-1} a^\star_j \cdot 2^j, b^\star = \sum_{j=0}^{n-1} b^\star_j \cdot 2^j)$. Let $\tilde{y}^\star = \sum_{j=0}^{n-1} \tilde{y}^\star_j \cdot 2^j$ denote the corresponding output with respect to Eq. (7). Given a set of $(a_{i+k}, b_{i+k}, a'_{i+k}, b'_{i+k}, a^\star_{i+k}, b^\star_{i+k})$, one can get $(c_{i+k+1}, \tilde{y}_{i+k+1}, c'_{i+k+1}, \tilde{y}'_{i+k+1}, c^\star_{i+k+1}, \tilde{y}^\star_{i+k+1})$ from $(c_{i+k}, \tilde{y}_{i+k}, c'_{i+k}, \tilde{y}'_{i+k}, c^\star_{i+k}, \tilde{y}^\star_{i+k})$ and value of x_{i+k}, where $i, k \in \mathbb{Z}$. Let arrows of plain head and "V-back" head denote $x_{i+k} = 0$ and $x_{i+k} = 1$ respectively, Figure 1 illustrates mapping relationship between $(c_{i+k}, \tilde{y}_{i+k}, c'_{i+k}, \tilde{y}'_{i+k}, c^\star_{i+k}, \tilde{y}^\star_{i+k})$ and $(c_{i+k+1}, \tilde{y}_{i+k+1}, c'_{i+k+1}, \tilde{y}'_{i+k+1}, c^\star_{i+k+1}, \tilde{y}^\star_{i+k+1})$ for a given $(a_{i+k}, b_{i+k}, a'_{i+k}, b'_{i+k}, a^\star_{i+k}, b^\star_{i+k})$, where $k = 0, 1, 2$. Since $(c_0, \tilde{y}_0, c'_0, \tilde{y}'_0, c^\star_0, \tilde{y}^\star_0) \equiv (0, 0, 0, 0, 0, 0)$, the dashed arrows in Fig. 1 describe Eq. (8) with the three sets of (a, b) for $i = 0, 1, 2$. Note that the data in the fourth column of the table shown in Fig. 1 is exactly the same as the first one. Therefore, Fig. 1 shows calculation of Eq. (7) under all different bit levels if the variable i shown in Fig. 1 go through $3 \cdot t$, where $t = 0 \sim \lfloor n/3 \rfloor$ and $i + k \leq n - 1$. From Fig. 1, it can be easily verified that the following relationship

$$\left(a_{i+k} + b_{i+k} \cdot 2 + \tilde{y}_{i+k} \cdot 2^2, a'_{i+k} + b'_{i+k} \cdot 2 + \tilde{y}'_{i+k} \cdot 2^2, a^\star_{i+k} + b^\star_{i+k} \cdot 2 + \tilde{y}^\star_{i+k} \cdot 2^2\right) \cap \{1, 2, 4, 7\} \neq \emptyset \tag{11}$$

is always satisfied, which means x_{i+k} can be derived from Table 3.1. This completes the proof.

■

Corollary 3.1. *The $(n-1)$ least significant bits of x in Eq. (6) can be determined easily by setting (a, b)*

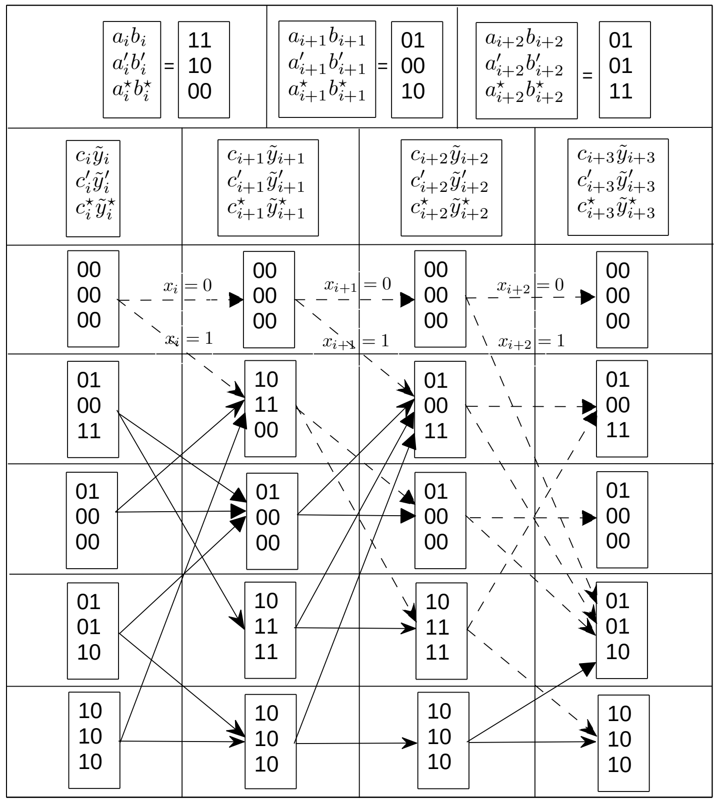

Fig. 1. Relationship between $(c_{i+k}, \tilde{y}_{i+k}, c'_{i+k}, \tilde{y}'_{i+k}, c^\star_{i+k}, \tilde{y}^\star_{i+k})$ and $(c_{i+k+1}, \tilde{y}_{i+k+1}, c'_{i+k+1}, \tilde{y}'_{i+k+1}, c^\star_{i+k+1}, \tilde{y}^\star_{i+k+1})$ for a given $(a_{i+k}, b_{i+k}, a'_{i+k}, b'_{i+k}, a^\star_{i+k}, b^\star_{i+k})$, where $k = 0, 1, 2$.

with the following three sets of numbers

$$\left\{\left(\sum_{j=0}^{\lceil n/3\rceil-1}(100)_2\cdot 8^j\right) \bmod 2^n, \left(\sum_{j=0}^{\lceil n/3\rceil-1}(111)_2\cdot 8^j\right) \bmod 2^n\right\};$$
$$\left\{\left(\sum_{j=0}^{\lceil n/3\rceil-1}(100)_2\cdot 8^j\right) \bmod 2^n, \left(\sum_{j=0}^{\lceil n/3\rceil-1}(001)_2\cdot 8^j\right) \bmod 2^n\right\};$$
$$\left\{\left(\sum_{j=0}^{\lceil n/3\rceil-1}(011)_2\cdot 8^j\right) \bmod 2^n, \left(\sum_{j=0}^{\lceil n/3\rceil-1}(001)_2\cdot 8^j\right) \bmod 2^n\right\}$$

and checking the corresponding $\tilde{y} = y \oplus a \oplus b$.

Proof. The proof is straightforward. ∎

Proposition 1. *Assume that a and x are both n-bit integers, $n \in \mathbb{Z}^+$, one has the following two equations*

$$(a \oplus x)\dot{-}x = (a \oplus x \oplus 2^{n-1})\dot{-}(x \oplus 2^{n-1}),$$
$$(a \oplus \overline{x})\dot{-}x = (a \oplus \overline{x \oplus 2^{n-1}})\dot{-}(x \oplus 2^{n-1}).$$

Proof. Eq. (12) can be proved under four conditions. i) When $(a \oplus x) \geq 2^{n-1}$ and $x \geq 2^{n-1}$: $(a \oplus x \oplus 2^{n-1})\dot{-}(x \oplus 2^{n-1}) = ((a \oplus x) - 2^{n-1})\dot{-}(x - 2^{n-1}) = (((a \oplus x) - 2^{n-1}) - (x - 2^{n-1}) + 2^n) \bmod 2^n = (a \oplus x)\dot{-}x$; ii) When $(a \oplus x) \geq 2^{n-1}$ and $x < 2^{n-1}$: $(a \oplus x \oplus 2^{n-1})\dot{-}(x \oplus 2^{n-1}) = ((a \oplus x) - 2^{n-1})\dot{-}(x + 2^{n-1}) = (((a \oplus x) - 2^{n-1}) - (x + 2^{n-1}) + 2^n) \bmod 2^n = (a \oplus x)\dot{-}x$; iii) When $(a \oplus x) < 2^{n-1}$ and $x \geq 2^{n-1}$: $(a \oplus x \oplus 2^{n-1})\dot{-}(x \oplus 2^{n-1}) = ((a \oplus x) + 2^{n-1})\dot{-}(x - 2^{n-1}) = (a \oplus x)\dot{-}x$; iv) When $(a \oplus x) < 2^{n-1}$ and $x < 2^{n-1}$: $(a \oplus x \oplus 2^{n-1})\dot{-}(x \oplus 2^{n-1}) = ((a \oplus x) + 2^{n-1})\dot{-}(x + 2^{n-1}) = (a \oplus x)\dot{-}x$. Similarly, Eq. (12) can be proved. ∎

Corollary 3.1 means that one can only choose four intermediate sequences, $\boldsymbol{J}_0$, $\boldsymbol{J}_1$, $\boldsymbol{J}_2$ and $\boldsymbol{J}_3$, to break MCKBA, where

$$\begin{aligned} J_0(i) &\equiv (\sum\nolimits_{j=0}^{\lceil n/3\rceil-1} 1\cdot 8^j) \bmod 2^n, \\ J_1(i) &\equiv (\sum\nolimits_{j=0}^{\lceil n/3\rceil-1} 7\cdot 8^j) \bmod 2^n, \\ J_2(i) &\equiv (\sum\nolimits_{j=0}^{\lceil n/3\rceil-1} 4\cdot 8^j) \bmod 2^n, \\ J_3(i) &\equiv (\sum\nolimits_{j=0}^{\lceil n/3\rceil-1} 6\cdot 8^j) \bmod 2^n. \end{aligned} \tag{12}$$

With respect to the 1D representation of 2D images defined in Sec. 2, basic repeated pattern of the corresponding gray-scale images of $\boldsymbol{J}_0$, $\boldsymbol{J}_1$, $\boldsymbol{J}_2$ and $\boldsymbol{J}_3$ are $[73, 146, 36]$, $[255, 255, 255]$, $[36, 73, 146]$, $[182, 109, 219]$, respectively. As shown in Proposition 1, the unknown most significant bits of key_1 and/or key_2 have no influence on decryption of MCKBA, so they are considered being recovered correctly in rest of the paper. Let $key^*(i)$ denote solution of Eq. (5) for $i = 0 \sim MN/(2n) - 1$, then $\{key^*(i)\}_{i=0}^{MN/(2n)-1}$ can be used as an equivalent key to decrypt any cipher-images of smaller size, encrypted with the same secret key.

The complexity of the differential attack is mainly determined by verifying the $n-1$ bits of each element in $\{key^*(i)\}_{i=0}^{MN/(2n)-1}$ from Table 3.1, so the complexity is proportional to the size of the plain-image.

3.2. *Breaking the Secret Key*

The differential attack described in the above subsection only outputs an equivalent key. We will show that the secret key can be further derived from it.

Assume $\{b(l)\}$ distributes over $\{0, 1\}$ uniformly, the probability $key_1 \notin (key^*(i))_{i=0}^{8MN/n-1}$ or $key_2 \notin (key^*(i))_{i=0}^{8MN/n-1}$ is $(1/2)^{8MN/n}$. So, we can obtain set (key_1, key_2) with a very high probability $1 - (1/2)^{8MN/n-1}$. Since $\sum_{j=0}^{n-2}(key_{1,j}\cdot 2^j) \neq \sum_{j=0}^{n-2}(key_{2,j}\cdot 2^j)$, one can narrow the scope of $B(i)$ from Eq. (5) as follows

$$B(i) \in \begin{cases} \{2, 3\}, & \text{if } \sum_{j=0}^{n-2}(key^*(i)_j \cdot 2^j) = \sum_{j=0}^{n-2}(key_{1,j}\cdot 2^j), \\ \{0, 1\}, & \text{if } \sum_{j=0}^{n-2}(key^*(i)_j \cdot 2^j) = \sum_{j=0}^{n-2}(key_{2,j}\cdot 2^j), \end{cases} \tag{13}$$

where $key^*(i) = \sum_{j=0}^{n-1}(key^*(i)_j \cdot 2^j)$ and $key^*(i) = \sum_{j=0}^{n-1}(key^*(i)_j \cdot 2^j)$.

Proposition 2. *Assume that a and x are both n-bit integers, $n \in \mathbb{Z}^+$, if a is odd, then $p = ((a \dotplus x) \oplus x)$ is always odd and $q = ((a \dotplus x) \odot x)$ is always even.*

Proof. This proposition can be proved by two equations

$$\begin{aligned} ((1 + x_0) \bmod 2) \oplus x_0 &\equiv 1, \\ ((1 + x_0) \bmod 2) \odot x_0 &\equiv 0. \end{aligned}$$

■

From Proposition 2 and Eq. (2), one can narrow the scope of $B(i)$ also according to encryption result of the second chosen intermediate sequence shown in Eq. (12), as follows

$$B(i) \in \begin{cases} \{1, 3\}, & \text{if } J_1'(i) \text{ is odd}, \\ \{0, 2\}, & \text{if } J_1'(i) \text{ is even}. \end{cases} \tag{14}$$

Once key_1 and key_2 are determined, value of $B(i)$, for $i = 0 \sim 8MN/n - 1$, can be determined exactly from Eq. (13) and Eq. (14). There are only two possible combinations of key_1 and key_2. If the searched version is the right one, $\{B(i)\}_{i=0}^{8MN/n-1}$ can be constructed correctly. Let $\{B^\star(i)\}_{i=0}^{8MN/n-1}$ and $\{B^*(i)\}_{i=0}^{8MN/n-1}$ denote the obtained version of $\{B(i)\}_{i=0}^{8MN/n-1}$ corresponding to the two combinations of

key_1 and key_2. Since Eq. (14) is unrelated with key_1 and key_2, one can assure that $B^\star(i) = B^*(i) \oplus 2$, i.e, $b^\star(2i) = 1 - b^*(2i)$ and $b^\star(2i+1) = b^*(2i+1)$, for $i = 0 \sim 8MN/n - 1$. Construct $\{x^\star(i)\}_{i=0}^{MN/(2n)-1}$ and $\{x^*(i)\}_{i=0}^{MN/(2n)-1}$, where $x^\star(i) = \sum_{j=1}^{32} b^\star(32 \cdot i + j - 1) \cdot 2^{-j}$, $x^*(i) = \sum_{j=1}^{32} b^*(32 \cdot i + j - 1) \cdot 2^{-j}$.

Since $\{x(i)\}_{i=0}^{MN/(2n)-1}$ come from consecutive chaotic states generated by iterating Logistic map, we can distinguish $\{x^\star(i)\}_{i=0}^{MN/(2n)-1}$ or $\{x^*(i)\}_{i=0}^{MN/(2n)-1}$ is the right sequence controlling encryption process, and verify key_1 and key_2 correspondingly, by checking whether any two consecutive elements of them satisfy specific correlation. As shown in [Rao & Gangadhar, 2007, Table 3], Eq. (1) is realized in 32-bit fixed-point arithmetic precision. So MCKBA satisfies condition described in Proposition 3. The whole secret key of MCKBA can be verified by checking whether some consecutive elements in $\{x^\star(i)\}_{i=0}^{MN/(2n)-1}$ and $\{x^*(i)\}_{i=0}^{MN/(2n)-1}$ satisfy Eq. (15). Finally, key_1, key_2, and $x(0) = \sum_{j=1}^{32} b(j-1) \cdot 2^j$ can be recovered. For HCKBA, we have to check which sequence agrees with distribution of the chaotic states generated by the hyperchaos generator like [Gangadhar & Rao, 2010, Fig. 6].

Proposition 3. *Assume that the Logistic map $x(k+1) = \mu \cdot x(k) \cdot (1 - x(k))$ is iterated with L-bit fixed-point arithmetic and that $x(k+1) \geq 2^{-m}$, where $1 \leq m \leq L$. Then, the following inequality holds*

$$|\mu - \tilde{\mu}_k| \leq 2^{m+3}/2^L, \tag{15}$$

where $\tilde{\mu}_k = \frac{x(k+1)}{x(k)\cdot(1-x(k))}$.

Proof. See appendix of [Li *et al.*, 2008b]. ■

3.3. *Experimental Results*

To verify the real performance of the above analysis, some experiments are carried out on some plain-images of size 512×512 when $n = 32$. The four chosen plain-images are shown in Fig. 2. When $x_0 = 319684607/2^{32}$, $key_1 = 3835288501$, and $key_2 = 1437224678$, the encryption results of the four chosen-image are shown in Fig. 3. Equivalent key $\{key^*(i)\}_{i=0}^{MN/(2n)-1}$ is used to decrypt another cipher-image shown in Fig. 4a) and the recovered result is shown in Fig. 4b). Three parts of the whole secret key, key_1, key_2 and the 32 bits of $x(0)$ can be verified by checking only three pairs of consecutive elements in $\{x^\star(i)\}_{i=0}^{MN/(2n)-1}$ and $\{x^*(i)\}_{i=0}^{MN/(2n)-1}$.

3.4. *Some Remarks on the Performance of MCKBA*

- Insufficient randomness of PRBS $\{b(l)\}$
  It is well-known that distribution of chaotic states generated by iterating Logistic map is not uniform, which makes randomness of derived binary bit sequence from them very low. As this point has been shown quantitatively in [Li *et al.*, 2007, 2010], detailed discussion is omitted here.
- Insensitivity with respect to changes of plain-image
  This defect may cause serious threat for any secure image encryption algorithm since image and its watermarked version may be encrypted at the same time. From Eq. (2), one can see that change of the m-th significant bit of $J(i)$ may only change the $m \sim (n-1)$-th significant bits of $J'(i)$, where $0 \leq m < n$. This means MCKBA can make change of one bit of plain-image to influence at most n bits in the corresponding cipher-image.
- Insensitivity with respect to changes of two sub-keys
  Obviously, any secure encryption algorithm should avoid this defect. Unfortunately, MCKBA is seriously fragile in this aspect. From Eq. (2), one can see that change of one bit of key_1 or key_2 only influences one bit of the corresponding cipher-image.

4. Conclusion

In this paper, security of the image encryption algorithm MCKBA has been studied in detail. It was found that the whole secret key can be recovered correctly with only four chosen plain-images. In addition, some

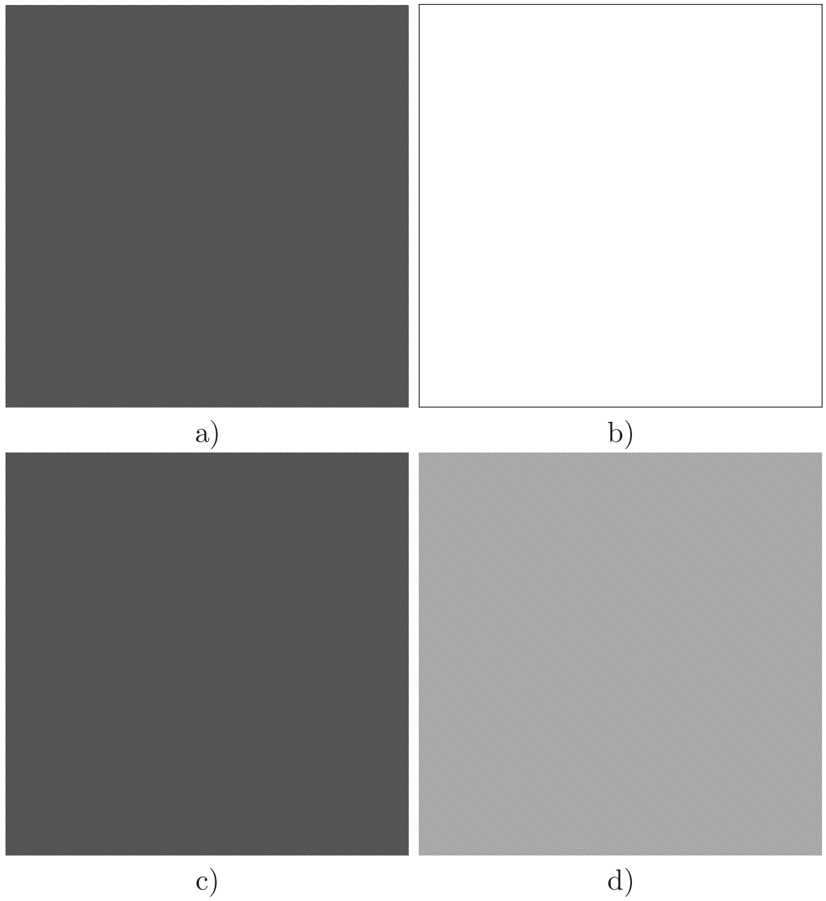

Fig. 2. Four chosen plain-images (The black boundary of Fig. 2b) is not its part).

other defects of the algorithm, including insensitivity with respect to changes of plain-image/secret key, were discussed. Analogue of MCKBA, HCKBA, have the same security problems. Due to such a low level of security provided by the two schemes (essentially one scheme), their application in practice should be performed with extreme caution.

Acknowledgement

This research was supported by The Hong Kong Polytechnic University's Postdoctoral Fellowships Scheme under grant no. G-YX2L.

References

Álvarez, G. & Li, S. [2006] "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos* **16**, 2129–2151.

Arroyo, D., Rhouma, R., Alvarez, G., Li, S. & Fernandez, V. [2008] "On the security of a new image encryption scheme based on chaotic map lattices," *Chaos* **18**, art. no. 033112.

Chen, G., Mao, Y. & Chui, C. K. [2004] "A symmetric image encryption scheme based on 3D chaotic cat maps," *Chaos, Solitons & Fractals* **21**, 749–761.

Chen, H.-C. & Yen, J.-C. [2003] "A new cryptography system and its VLSI realization," *Journal of Systems Architecture* **49**, 355–367.

Ercan, S. & Cahit, C. [2009] "Algebraic break of a cryptosystem based on discretized two-dimensional chaotic maps," *Physics Letters A* **373**, 1352–1356.

Gangadhar, C. & Rao, K. D. [2010] "Hyperchaos based image encryption," *International Journal of Bifurcation and Chaos* **19**, 3833–3839.

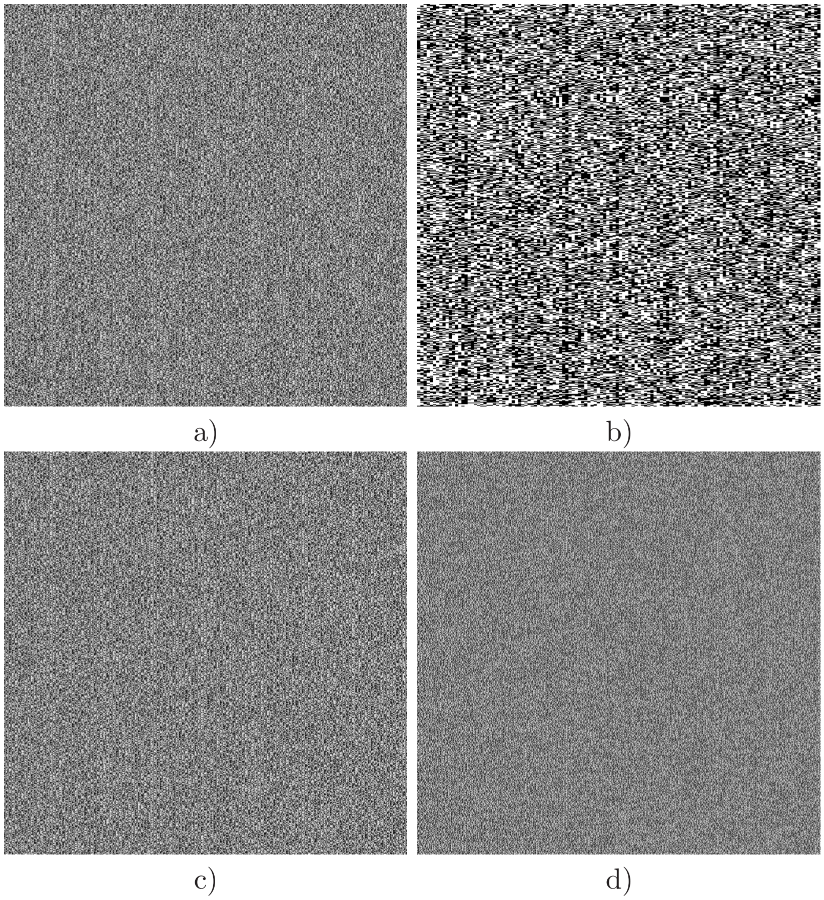

Fig. 3. The corresponding cipher-images of the four chosen plain-images shown in Fig. 2.

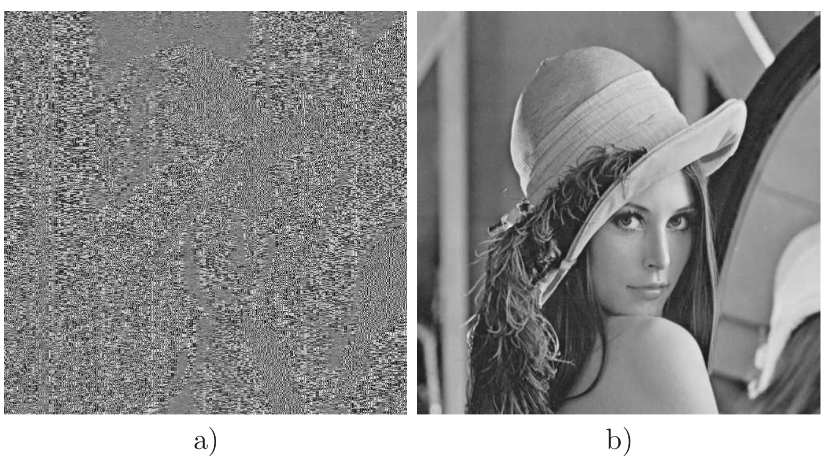

Fig. 4. The decryption result of another cipher-image encrypted with the same secret key: a) cipher-image; b) decrypted plain-image.

Li, C., Li, S., Álvarez, G., Chen, G. & Lo, K.-T. [2007] "Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations," *Physics Letters A* **369**, 23–30.

Li, C., Li, S., Asim, M., Nunez, J., Alvarez, G. & Chen, G. [2009a] "On the security defects of an image encryption scheme," *Image and Vision Computing* **27**, 1371–1381.

Li, C., Li, S., Chen, G. & Halang, W. A. [2009b] "Cryptanalysis of an image encryption scheme based on a compound chaotic sequence," *Image and Vision Computing* **27**, 1035–1039.

Li, C., Li, S. & Lo, K.-T. [2010] "Breaking a modified substitution-diffusion image cipher based on chaotic

standard and logistic maps," doi:10.1016/j.cnsns.2010.05.008.

Li, S., Chen, G. & Zheng, X. [2004] "4," *Chaos-Based Encryption for Digital Images and Videos*, Multimedia Security Handbook (CRC Press), pp. 133–167.

Li, S., Li, C., Chen, G., Bourbakis, N. G. & Lo, K.-T. [2008a] "A general quantitative cryptanalysis of permutation-only multimedia ciphers against plaintext attacks," *Signal Processing: Image Communication* **23**, 212–223.

Li, S., Li, C., Chen, G. & Lo, K.-T. [2008b] "Cryptanalysis of the RCES/RSES image encryption scheme," *Journal of Systems and Software* **81**, 1130–1143.

Li, S. & Zheng, X. [2002] "Cryptanalysis of a chaotic image encryption method," *Proc. IEEE International Symposium on Circuits and Systems*, pp. 708–711.

Pisarchik, A. N., Flores-Carmona, N. J. & Carpio-Valadez, M. [2006] "Encryption and decryption of images with chaotic map lattices," *Chaos* **16**, art. no. 033118.

Rao, K. & Gangadhar, C. [2007] "Modified chaotic key-based algorithm for image encryption and its VLSI realization," *Proceedings of the 2007 15th International Conference on Digital Signal Processing*, pp. 439–442.

Socek, D., Li, S., Magliveras, S. S. & Furht, B. [2005] "Enhanced 1-D chaotic key-based algorithm for image encryption," *Proceedings of the First IEEE/CreateNet International Conference on Security and Privacy for Emerging Areas in Communication Networks (SecureComm 2005)*, pp. 406–408.

Solak, E., Cokal, C., Yildiz, O. T. & Biyikoglu, T. [2010] "Cryptanalysis of Fridrich's chaotic image encryption," *International Journal of Bifurcation and Chaos* **20**, 1405–1413.

Takahashi, Y., Nakano, H. & Saito, T. [2004] "A simple hyperchaos generator based on impulsive switching," *IEEE Transactions on Circuits and Systems II-Express Briefs* **51**, 468–472.

Wang, K., Pei, W., Zou, L., Song, A. & He, Z. [2005] "On the security of 3D cat map based symmetric image encryption scheme," *Physics Letters A* **343**, 432–439.

Wong, K.-W., Lin, Q. & Chen, J. [2010] "Simultaneous arithmetic coding and encryption using chaotic maps," *IEEE Transactions on Circuits and Systems II-Express Briefs* **57**, 146–150.

Xiang, T., Wong, K.-W. & Liao, X. [2007] "A novel symmetrical cryptosystem based on discretized two-dimensional chaotic map," *Physics Letters A* **364**, 252–258.

Ye, G. [2010] "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognition Letters* **31**, 347–354.

Yen, J.-C. & Guo, J.-I. [2000] "A new chaotic key-based design for image encryption and decryption," *Proceedings of IEEE International Symposium on Circuits and Systems*, pp. 49–52.

Zhou, J. & Au, O. C. [2008] "Comments on "a novel compression and encryption scheme using variable model arithmetic coding and coupled chaotic system"," *IEEE Transactions on Circuits and Systems I* **55**, 3368–3369.